Marked-up version of the amended claims--additions are shown with double-underlines and deletions are shown with strike-throughs.

1. A method of enabling a proxy to participate in a secure communication between a client and a server, comprising the step of:

establishing a first secure session between the client and the proxy;

upon verifying the first secure session, establishing a second secure session between the client and the proxy, the second secure session requesting the proxy to act as a conduit to the server;

having the client and the server negotiate a session master secret; and

delivering the session master secret to the proxy using the first secure session to enable the proxy to participate in the secure communication.

2. The method as described in claim 1 further including the step of having the proxy use the session master secret and a session identifier to generate given cryptographic information.

3. (Amended) The method as described in claim 2 further including the step of having the proxy modify requests and responses ~~enter an active operating state~~ following receipt of the session master secret and generation of the given cryptographic information.

4. (Amended) The method as described in claim 3 wherein the proxy performs a given service on behalf of the client while modifying content from the server. ~~in the active operating state.~~

5. The method as described in claim 4 wherein the given service is selected from a set of services including transcoding, caching, encryption, decryption, monitoring, filtering and pre-fetching.

6. The method as described in claim 1 wherein the first and second secure sessions confirm to a network security protocol.

7. The method as described in claim 6 wherein the network security protocol is SSL.

8. The method as described in claim 6 wherein the network security protocol is TLS.

9. The method as described in claim 1 wherein the server is a Web server and the client is a pervasive computing client.

10. A method of enabling a proxy to participate in a secure communication between a client and a server, comprising the step of:

having the client request a first secure connection to the proxy;

upon authenticating validity of a certificate received from the proxy, having the client request a second secure connection to proxy, the second secure connection requesting the proxy to act as a conduit to the server;

having the proxy generate a session identifier;

having the client and the server negotiate a session master secret through the conduit;

upon completion of the negotiation, having the client deliver the session master secret to the proxy using the first secure connection;

having the proxy use the session master secret and the session identifier to generate given cryptographic information that is useful for participating in the secure communication.

11. (Amended) The method as described in claim 10 further including the step of having the proxy modify requests and

responses ~~enter an active operating state~~ following receipt of the session master secret and generation of the given cryptographic information.

12. (Amended) The method as described in claim 11 wherein the proxy performs a given service on behalf of the client while modifying content from the server. ~~in the active operating state.~~

13. The method as described in claim 12 wherein the given service is selected from a set of services including transcoding, caching, encryption, decryption, monitoring, filtering and pre-fetching.

14. The method as described in claim 10 wherein the first and second secure sessions confirm to a network security protocol.

15. The method as described in claim 14 wherein the network security protocol is SSL.

16. The method as described in claim 14 wherein the network security protocol is TLS.

17. A method for establishing the security of a session between a client and a server, comprising the steps of:

through a proxy, conducting a security handshake procedure between the client and the server to produce a session key; and

transmitting the session key to the proxy so that the proxy can participate in communications between the client and the server during the session.

18. The method as described in claim 17 wherein the session key is transmitted from the client to the proxy over a secure connection.

19. The method as described in claim 18 wherein the secure connection between the client and the proxy is created before the security handshake procedure and is maintained throughout the session.

20. (Amended) A cryptographic system, comprising:

a client;

a server;

a proxy;

a network protocol service for enabling the client and server to communicate over a secure connection;

a computer program (i) for controlling the client to request a first secure connection to the proxy, (ii)

responsive to authenticating validity of a certificate from the proxy, for controlling the client to request a second secure connection to proxy, the second secure connection requesting the proxy to act as a conduit to the server, (iii) for controlling the client to negotiate with the server through the conduit to obtain a session master; and (iv) upon successful completion of the negotiation, for controlling the client to deliver the session master secret to the proxy using the first secure connection; and

a computer program (i) for controlling the proxy to use the session master secret and a session identifier to generate given cryptographic information, and (ii) for having ~~switching~~ the proxy modify content ~~into an active operating state during which it can participate~~ in communications between the client and the server.

21. The cryptographic system as described in claim 20 wherein the proxy includes means for providing transcoding services on behalf of the client.

22. The cryptographic system as described in claim 20 wherein the proxy includes means for providing encryption/decryption services on behalf of the client.

23. The cryptographic system as described in claim 20 wherein the proxy includes means for providing caching services on behalf of the client.

24. The cryptographic system as described in claim 20 wherein the proxy includes means for providing monitoring services on behalf of the client.

25. (Amended) A computer program product in a computer readable medium for use in a cryptographic system including a client, a server, and a proxy, comprising:

a first routine (i) for controlling the client to request a first secure connection to the proxy, (ii) responsive to authenticating validity of a certificate from the proxy, for controlling the client to request a second secure connection to proxy, the second secure connection requesting the proxy to act as a conduit to the server, (iii) for controlling the client to negotiate with the server through the conduit to obtain a session master; and (iv) upon successful completion of the negotiation, for controlling the client to deliver the session master secret to the proxy using the first secure connection; and

a second routine (i) for controlling the proxy to use the session master secret and a session identifier to generate given cryptographic information, and (ii) for having ~~switching~~

the proxy modify content ~~into an active operating state during which it can participate~~ in communications between the client and the server.

II. Amendments to the Specification

Please amend the specification as follows with the following clean versions of the amended paragraphs in accordance with 37 CFR § 1.121; marked-up versions of the paragraphs are presented in the following section.

Clean version of amended paragraphs:

On page 10, lines 6-21:

The above-described functionality is known in the art. The functionality is implemented, for example, in protocols confirming to IETF TLS Version 1.0 and SSL Version 2.0/3.0. These protocols, while very similar, are composed of two layers: the record protocol and the handshake protocol. As will be seen, the present invention provides a method of extending these types of security protocols to extend the privacy of a session to a third party intermediary or proxy. Preferably, the invention is implemented as a handshake protocol between a client and a proxy that is layered on top of a secure session, as will be seen. This extension does not change the basic properties of the secure connection at the record protocol layer. Although the technique is described in the context of TLS and SSL, this is not a limitation of the present invention.

Marked-up version of the amended paragraphs--additions are shown with double-underlines and deletions are shown with strike-throughs.

On page 10, lines 6-21:

The above-described functionality is known in the art. The functionality is implemented, for example, in protocols confirming to IETF TLS Version 1.0 and SSL Version 2.0/3.0. These protocols, while very similar, are composed of two layers: the record protocol and the handshake protocol. As will be seen, the present invention provides a method of extending these types of security protocols to extend the privacy of a session to a third party intermediary or proxy. Preferably, the invention is implemented as a handshake protocol between a client and a proxy that is layered on top of a secure session, as will be seen. This extension does not change the basic properties of the secure connection at the record protocol layer. Although the technique is described in the context of TLS ~~TLS~~ and SSL, this is not a limitation of the present invention.

III. General Remarks Concerning This Response

Claims 1-25 are currently pending in the present application. Depending on the manner in which one reads the 101 rejection and the 112 rejection, claims 1-9 or claims 1-13 may be rejected; claims 1 and 6-9 are rejected over prior art. Claims 3, 4, 11, 12, 20, and 25 have been amended in this response; no claims have been added or canceled. Reconsideration of the claims is respectfully requested.

The Office action contained an objection to the specification. In response, the specification has been amended to correct the typographical error.

The Office action contained an objection to the drawings. In response, a proposed drawing correction has been submitted at the end of this response.

IV. Summary of Present Invention

A method of enabling a proxy to participate in a secure communication between a client and a server. The method begins by establishing a first secure session between the client and the proxy. Upon verifying the first secure session, the method continues by establishing a second secure session between the client and the proxy. In the second secure session, the client requests the proxy to act as a conduit to the server. Thereafter, the client and the server negotiate a session master secret. Using the first secure session, this session master secret is then provided by the client to the proxy to enable the proxy to participate in secure communications between the client and the server. After receiving the session master secret, the proxy generates cryptographic information that enables it to provide a given service (e.g., transcoding, monitoring, encryption/decryption, caching, or the like) on the client's behalf and without the

server's knowledge or participation. The first secure session is maintained between the client and the proxy during such communications.

V. 35 U.S.C. § 101–Utility

Although there are no claims listed in the rejection, a general rejection appears to be made about the claims. The rejection states the following:

> The detailed description of the claimed invention lacks patentable utility. On page 8, lines 14-15, of the specification, the application discloses that any given program may be capable of being both a client and a server. The examiner asserts that not every program is capable of being both a client and a server. Not all games and applications are capable of being a client or server.

The argument in the Office action seems to be directed more towards an enablement rejection than a utility rejection, but in any case, Applicant believes that the sentence in the specification appears to have been misinterpreted because the sentence states "any given program", not "every program" as restated within the rejection. In other words, Applicant agrees that not every program can act as both a client and a server; however, there are some programs that may act as both a client and a server. If Applicant had the opportunity, Applicant could present a particular program that has the described characteristics. Applicant asserts that the sentence is grammatically correct as stated in the specification for the meaning that was intended by Applicant.

VI. 35 U.S.C. § 112, ¶ 1–Enablement

Claims 3-5 and 11-13 are rejected under 35 U.S.C. § 112, ¶ 1, as based on a disclosure which is not enabling. The rejection states the following:

> Applicant discloses the proxy entering an active operating state following receipt of the session master secret and generation of the given cryptographic information. There are not enough details in the specification for the examiner to understand how the proxy enters an active operating state following receipt of the session master secret and generation of the given cryptographic information. The examiner asserts that the proxy should already be in an active operating state to receive a session master secret and generate any given cryptographic information.

In response, Applicant has modified claims 3, 4, 11, 12, 20, and 25 to delete the term "active operating state" and to insert the term "modifying requests and responses" or the term "modifying content". The present application provides support for this amendment on page 14 of the specification. With respect to step 34 in FIG. 3, the specification states the proxy receives a session identifier and session master secret. With respect to step 38, the proxy may modify a request, and with respect to step 42, the proxy may modify the data in received content. Applicant asserts that the amendment obviates the rejection under 35 U.S.C. § 112, ¶ 1, and Applicant requests the withdrawal of the rejection.

VII. 35 U.S.C. § 103(a)—Obviousness

The Office action has rejected claim 1 under 35 U.S.C. § 103(a) as unpatentable over Vu, "Apparatus and method for providing a secure gateway for communication and data exchanges between networks", U.S. Patent No. 5,623,601, filed 11/21/1994, issued 04/22/1997, in view of Raivisto, "Method of implementing connection security in a wireless network", U.S. Patent Number 6,081,601, filed 01/27/1998, issued 06/27/2000. This rejection is respectfully traversed.

The beginning of the rejection of independent claim 1 states:

> As per claim 1, Vu discloses establishing a first secure connection between the client and the proxy (gateway station 14). Vu discloses that upon verifying the first secure session, establishing a second secure session between the client and the proxy (gateway station 14), the second secure session requesting the proxy to act as a conduit to the server, column 8 lines 54-64. Vu does not disclose having the client and the server negotiate a session master secret and delivering the session master secret to the proxy using the first secure session to enable the proxy to participate in the secure communication.

Vu clearly does not disclose some of the claimed features of the present invention, notwithstanding the arguments presented by the rejection. The portion of Vu that is cited by the rejection, column 8, lines 54-64, reads as follows:

> As will be explained below in detail, the process then authenticates the client's authorization to access the requested service and if the client 16 is determined to have the required authorization, the gateway station 14 initiates a second communication process 19 with the remote host 46 in which the gateway station 14 simulates the client 16 without revealing the client address. Once the two communication sessions 17, 19 are operative, communication is effected between the client 16 and the host 46 by passing communication data between the two interdependent communication sessions.

According to the rejection, the gateway in Vu is analogous to the proxy in the present application. The rejection states that Vu discloses at col. 8, lines 54-64, that there are two communication sessions between the client and the gateway, but Vu does not disclose this. Vu discloses two communication sessions: one between the host server and the gateway and the other session between the gateway and the client. Thus, in Vu, the gateway acts as an intermediary between the host and the client, and the client and the gateway communicate only through one communication session,

whereas in the present invention, the client and the proxy communicate through two communication sessions.

Independent claim 1 reads in its entirety:

> 1. A method of enabling a proxy to participate in a secure communication between a client and a server, comprising the step of:
> establishing a first secure session between the client and the proxy;
> upon verifying the first secure session, establishing a second secure session between the client and the proxy, the second secure session requesting the proxy to act as a conduit to the server;
> having the client and the server negotiate a session master secret; and
> delivering the session master secret to the proxy using the first secure session to enable the proxy to participate in the secure communication.

In the present application, after establishing a first communication session between the client and the proxy, the client then establishes a second communication session between the client and the proxy. The second communication session is established through the proxy such that the proxy acts as a conduit or tunnel. For this second communication session, the proxy merely transfers the content between the client and the server, and the proxy does not actively process the content, such as transcoding the content or some other function. After the client obtains a session master secret from the server through the second communication session, the client transfers the session master secret to the proxy using the first communication session, after which the client communicates with the server through the first communication session. The proxy and the client maintain the first secure session, and the server is unaware that it is communicating with the proxy using the session master secret rather than the client; in a typical, prior art case, the server would communicate directly with the client using the session master secret. With the

present invention, the proxy performs its active processing, such as transcoding content, with the message traffic through the first communication session. In addition, the entire communication channel remains secure with the server unaware that the proxy is acting as an intermediary between the client and the server.

Hence, the rejection of claim 1 contains a fundamental flaw in that it argues that Vu discloses two communications sessions between the proxy (gateway station in Vu) and the client, but this is incorrect. The rejection then proceeds to rely on Raivisto to remedy another deficiency in Vu with respect to the secure characteristic of the communication sessions in claim 1. However, Raivisto clearly discloses a similar arrangement of communication elements.

The rejection combines the teachings of Vu and Raivisto by stating: "A first secure connection will be made between a client (MS1) and a proxy (MD). A second connection will be made between a client (MS1) and a proxy (MD) that enables the proxy to act as a conduit to the server. Secret keys will be established [sic] the proxy (MD) and the client (MS1) and the proxy (MD) and the server (MS2)." This combination apparently argues that an analogy can be made between the proxy of the present invention and the mediator of Raivisto, but it does not explain how the prior art shows two communication sessions between a terminal/client and a mediator/gateway/proxy as claimed in the present invention.

In other words, the combination of Raivisto with Vu does not remedy the most prominent deficiency in Vu because the basic configuration of Raivisto is similar to Vu. In Raivisto, the mediator acts as an intermediary between two terminals; this configuration is analogous to the gateway acting as an intermediary between the host and the client in

Vu or the proxy acting as an intermediary between the server and the client in the present invention. However, Raivisto does not disclose two communication sessions between a single terminal and the mediator, as would be necessary before Raivisto can begin to disclose the claimed features of the present invention concerning two secure communication sessions between a client and a proxy.

The Office action proceeds to reject dependent claims 6-8 under 35 U.S.C. § 103(a) as unpatentable over Vu in view of Raivisto and further in view of Davis et al., U.S. Patent Number 6,367,009. This rejection is respectfully traversed.

Dependent claims 6-8 merely state that the secure sessions are based on particular network security protocols, such as SSL and TLS, and the rejection merely relies on Davis et al. as disclosing these protocols. However, claims 6-8 incorporate the features of independent claim 1, and Davis et al. does not teach the claim elements of independent claim 1 as discussed above. Hence, the rejection of claims 6-8 is also deficient as Davis et al. does not remedy the deficiencies of Vu and Raivisto concerning the two secure communication sessions between the client and the proxy as claimed.

The Office action proceeds to reject dependent claim 9 under 35 U.S.C. § 103(a) as unpatentable over Vu in view of Raivisto and further in view of Rosecrans et al., U.S. Patent Number 5,889,852. This rejection is respectfully traversed.

Dependent claim 9 merely states that the server is a Web server and that the client is a pervasive computing client, and the rejection merely relies on Rosecrans et al. as disclosing these features. However, claim 9 incorporates the features of independent claim 1, and Rosecrans et al. does not teach the claim elements of independent claim 1 as discussed

above. Hence, the rejection of claim 9 is also deficient as Rosecrans et al. does not remedy the deficiencies of Vu and Raivisto concerning the two secure communication sessions between the client and the proxy as claimed.

Examiner bears the burden of establishing a *prima facie* case of obviousness.

The examiner bears the burden of establishing a *prima facie* case of obviousness based on the prior art when rejecting claims under 35 U.S.C. § 103. *In re Fritch*, 972 F.2d 1260, 23 U.S.P.Q.2d 1780 (Fed. Cir. 1992). Only when a *prima facie* case of obviousness is established does the burden shift to the applicant to produce evidence of nonobviousness. *In re Oetiker*, 977 F.2d 1443, 1445, 24 U.S.P.Q.2d 1443, 1444 (Fed. Cir. 1992); *In re Rijckaert*, 9 F.3d 1531, 1532, 28 U.S.P.Q.2d 1955, 1956 (Fed. Cir. 1993). If the Patent Office does not produce a *prima facie* case of unpatentability, then without more the applicant is entitled to the grant of a patent. *In re Oetiker*, 977 F.2d 1443, 1445, 24 U.S.P.Q.2d 1443, 1444 (Fed. Cir. 1992); *In re Grabiak*, 769 F.2d 729, 733, 226 U.S.P.Q. 870, 873 (Fed. Cir. 1985). In response to an assertion of obviousness by the Patent Office, the applicant may attack the Patent Office's *prima facie* determination as improperly made out, present objective evidence tending to support a conclusion of nonobviousness, or both. *In re Fritch*, 972 F.2d 1260, 1265, 23 U.S.P.Q.2d 1780, 1783 (Fed. Cir. 1992).

With respect to claims 1 and 6-9, Vu in view of Raivisto and further in view of David et al. or Rosecrans et al. does not disclose the claimed invention nor provide any suggestion to motivate one having ordinary skill in the art to modify the prior art to reach the claimed invention. In fact, the

rejection appears to disregard entire claim elements without justification. In general, the rejection does not point out the necessary teachings, suggestions, or incentives to reach the claimed invention. Hence, the rejection of claims 1 and 6-9 does not establish a *prima facie* case of obviousness based on the prior art. Therefore, the rejection of claims 1 and 6-9 under 35 U.S.C. § 103(a) has been shown to be insupportable, and these claims are patentable over the applied prior art. Applicant requests the withdrawal of the rejection.

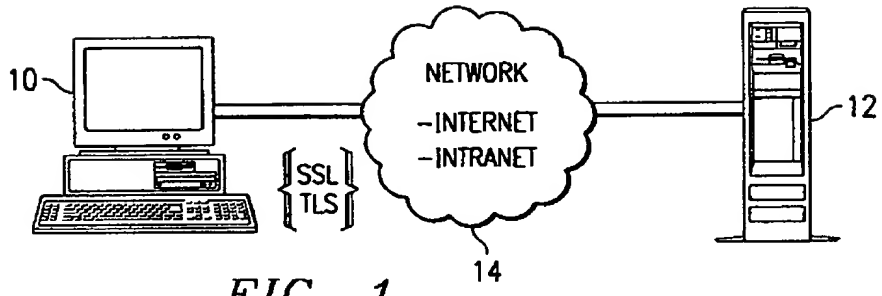


FIG. 1
(Prior Art)

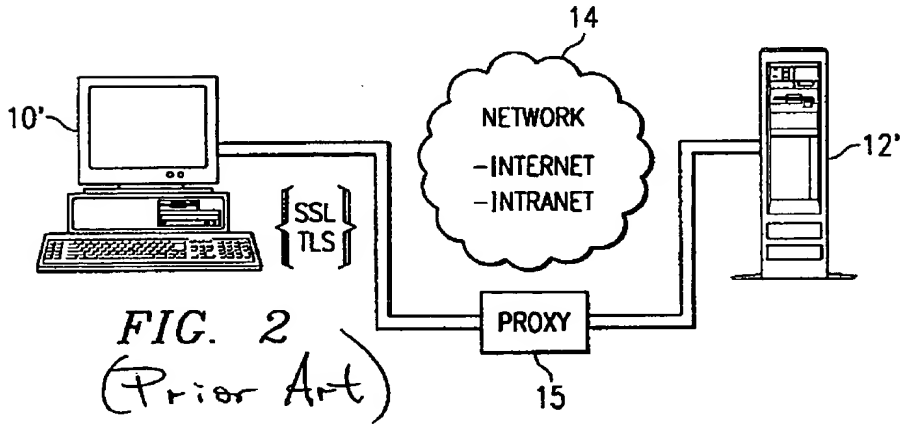


FIG. 2
(Prior Art)

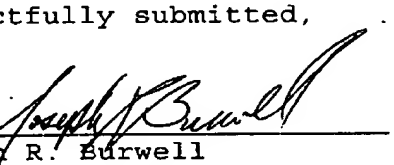
VIII. Conclusion

It is respectfully urged that the present patent application is patentable, and Applicant kindly requests a Notice of Allowance.

For any other outstanding matters or issues, the examiner is urged to call or fax the below-listed telephone numbers to expedite the prosecution and examination of this application.

DATE: March 31, 2003

Respectfully submitted,



Joseph R. Burwell
Reg. No. 44,468
ATTORNEY FOR APPLICANT

Law Office of Joseph R. Burwell
P.O. Box 28022
Austin, Texas 78755-8022
Voice: 866-728-3688 (866-PATENT8)
Fax: 866-728-3680 (866-PATENT0)
Email: joe@burwell.biz